(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 35 019 A 1**

(51) Int. Cl.[6]:
G 11 B 5/70
G 11 B 23/28
// G07C 9/00,G07F 7/08

(21) Aktenzeichen: 195 35 019.7
(22) Anmeldetag: 21. 9. 95
(43) Offenlegungstag: 27. 3. 97

(71) Anmelder:
CardTec Entwicklungs- und Vertriebsgesellschaft für elektronische Kartensysteme mbH, 44795 Bochum, DE

(74) Vertreter:
Schneiders · Behrendt · Finkener · Ernesti, Rechtsanwälte · Patentanwälte, European Patent Attorneys, 44787 Bochum

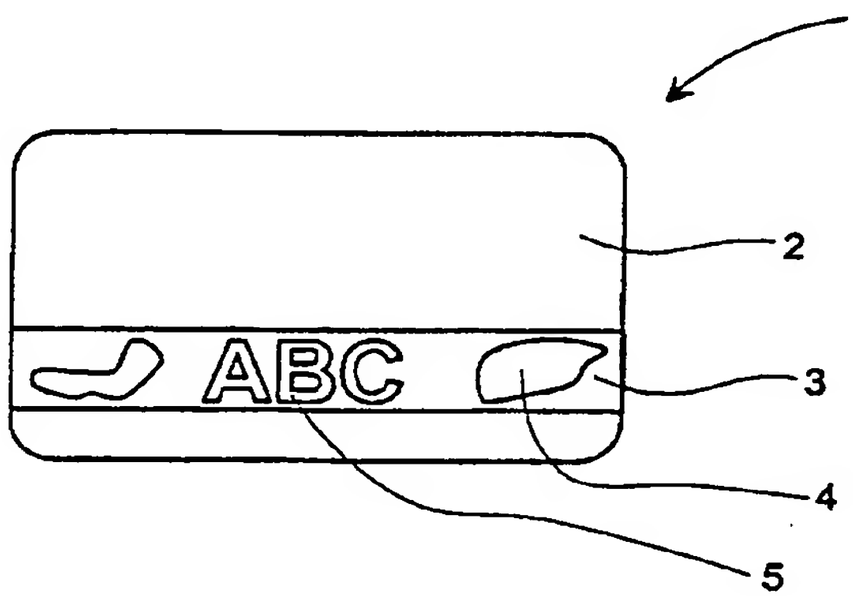
(72) Erfinder:
Künstler, Rainer, 44795 Bochum, DE

(56) Entgegenhaltungen:
DE 36 17 319 C2
DE 37 05 006 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Magnetisches Speichermedium mit verschlüsselten Rohdaten

(57) Die vorliegende Erfindung betrifft ein magnetisches Speichermedium, insbesondere eine Magnetkarte (1) mit einem Magnetstreifen (3), auf dem Rohdaten mit einem bestimmten Informationsgehalt in verschlüsselter Form abgespeichert sind. Um das Kopieren oder Fälschen solcher magnetischer Speichermedien wesentlich zu erschweren oder sogar unmöglich zu machen, schlägt die Erfindung vor, auf dem Magnetstreifen (3) ein beliebiges Muster (4, 5) aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens (3) abweichenden Koerzitivität aufzubringen. Vorteilhaft weist die Koerzitivität des magnetischen Materials des Musters (4, 5) ein Mehrfaches der Koerzitivität des Magnetstreifens (3) auf. Aus der Position und Ausdehnung des magnetischen Musters (4, 5) auf dem Magnetstreifen (3) und der Koerzitivität des Magnetstreifens (3) werden Entschlüsselungsinformationen ermittelt, mit deren Hilfe aus den verschlüsselten Daten die auf der Magnetkarte (1) gespeicherten Rohdaten extrahiert.



DE 195 35 019 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Beschreibung

Die vorliegende Erfindung betrifft ein magnetisches Speichermedium, insbesondere eine Magnetkarte mit einem Magnetstreifen, auf dem Rohdaten mit einem bestimmten Informationsgehalt in verschlüsselter Form abgespeichert sind.

Das Verschlüsseln von Rohdaten auf magnetischen Speichermedien ist notwendig, um unberechtigten Dritten den Zugang zu diesen Rohdaten zu erschweren oder unmöglich zu machen. Es gibt verschiedene Möglichkeiten, Magnetkarten illegal zu vervielfältigen.

Man kann beispielsweise die Daten einer Magnetkarte auf eine zweite kopieren. Dazu genügt eine relativ einfache Vorrichtung, bestehend aus einem Lesekopf und einem mit diesem über einen elektronischen Verstärker verbundenen Schreibkopf. Während der Lesekopf über den Magnetstreifen der einen Magnetkarte gleitet, speichert der Schreibkopf diese eingelesenen Daten gleichzeitig auf dem Magnetstreifen der zweiten Magnetkarte.

Dieses illegale Kopieren von Magnetkarten ist besonders bei Kreditkarten verbreitet. Mit diesen gefälschten Kreditkarten kann ein hoher Schaden angerichtet werden, da sie ohne zusätzliche Sicherheitsvorkehrungen (z. B. Geheimnummer, PIN) eingesetzt werden und sie für relativ große Geldbeträge einsetzbar sind.

Magnetkarten werden auch als Zugangskontrolle für Verkehrsmittel (Fahrscheine), Skilifte (Skipässe) oder Veranstaltungen (Eintrittskarten) verwendet.

Diese Magnetkarten für Fahrkarten, Skipässe oder Eintrittskarten bestehen aus einem flexiblen Trägermaterial aus Kunststoff oder Papier, auf welchem der Magnetstreifen aufgebracht ist, der die Rohdaten mit den Informationen (z. B. Ausstellungsort, Ausstellungsdatum, Gültigkeitsdauer) enthält. In zunehmendem Maße werden auch solche Magnetkarten illegal vervielfältigt, indem sie mittig entlang des Magnetstreifens in Längsrichtung durchschnitten werden. Diese halben Magnetstreifen werden auf Unterlagen geklebt, die die Größe der ursprünglichen Magnetkarten haben. Die Koerzitivität des halben Magnetstreifens reicht in den meisten Fällen aus, um vom Magnetkartenleser noch eingelesen werden zu können.

Aus der EP 0 313 063 A2 ist ein Verschlüsselungsverfahren bekannt, bei dem ein Muster aus einem magnetischen Material mit einer Koerzitivität, die kleiner als 30 Oersted ist, auf den Magnetstreifen aufgebracht ist. Die Position und die örtliche Ausdehnung des magnetischen Musters auf dem Magnetstreifen sind bekannt. Dieses Wissen wird beim Entschlüsseln der durch das magnetische Muster verschlüsselten, auf dem Magnetstreifen abgelegten Daten berücksichtigt. Die zum Entschlüsseln der Daten notwendigen Informationen müssen also in den Magnetkarten-Lesegeräten vorhanden sein. Um die Kompatibilität der einzelnen Magnetkarten mit den Magnetkarten-Lesegeräten gewährleisten zu können, müssen die einzelnen Magnetkarten mit dem gleichen magnetischen Muster verschlüsselt werden.

Es ist damit weiterhin möglich, den Inhalt solcher Magnetkarten mit einem einfachen Lese-/Schreibgerät von einer verschlüsselten Magnetkarte auf eine andere, ebenso verschlüsselte zu kopieren. Eine wesentliche Möglichkeit, Magnetkarten zu fälschen, wird durch dieses Verschlüsselungsverfahren nicht beseitigt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein magnetisches Speichermedium der eingangs genannten Art dahingehend weiterzubilden, daß das

Kopieren oder Fälschen wesentlich erschwert oder sogar unmöglich gemacht wird.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von dem magnetischen Speichermedium der eingangs genannten Art vor, daß auf dem Magnetstreifen ein beliebiges Muster aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens abweichenden Koerzitivität aufgebracht ist.

Die Erfindung macht es möglich, auf nahezu jede Magnetkarte ein individuelles Muster aufzubringen. Durch das Aufbringen eines solchen magnetischen Musters auf den Magnetstreifen ist die Koerzitivität des Magnetstreifens nicht mehr homogen, sondern weist inhomogene Eigenschaften auf.

Die unterschiedlichen Muster auf den Magnetkarten machen es überflüssig, daß die zur Entschlüsselung nötigen Informationen in dem Magnetkarten-Lesegerät vorhanden sind, da die Entschlüsselungsinformationen von Magnetkarte zu Magnetkarte variieren. Bei der Magnetkarte gemäß der Erfindung können die Informationen für die Entschlüsselung aus den auf dem Magnetstreifen enthaltenen Daten für jede Magnetkarte gesondert extrahiert werden.

Dies geschieht bei der erfindungsgemäßen Magnetkarten folgendermaßen: Die Rohdaten werden auf der Magnetkarte im allgemeinen mittels periodischer Flußwechsel des Magnetfeldes auf dem Magnetstreifen abgelegt. Bei Magnetkarten mit unverschlüsselten Daten und herkömmliche Magnetstreifen aus einem homogenen magnetischen Material konstanter Koerzitivität weisen die Amplituden des magnetischen Flusses eine konstante Größe auf. Bei Magnetkarten mit verschlüsselten Daten und Magnetstreifen, auf denen gemäß der Erfindung ein Muster aus einem magnetischen Material abweichender Koerzitivität aufgebracht ist, variieren die Amplituden des magnetischen Flusses abhängig von der unterschiedlichen Koerzitivität des Magnetstreifens. Aufgrund der unterschiedlichen Amplituden des magnetischen Flusses kann man abhängig von den periodischen Flußwechseln die absolute Position und Ausdehnung des Musters auf dem Magnetstreifen und die jeweilige Koerzitivität des Magnetstreifens ermitteln. Mit Hilfe dieser Informationen können aus dem im Lesekopf des Magnetkarten-Lesegerätes induzierten Spannungssignal die Rohdaten extrahiert werden.

Derart mit individuellen Mustern verschlüsselte Magnetkarten können folglich von einem einzigen Magnetkarten-Lesegerättyp eingelesen und entschlüsselt werden, ohne daß dieser vorher das Muster kennt.

Nach dem Einlesen und Entschlüsseln der Rohdaten werden diese manipuliert. Es kann beispielsweise die Verlängerung der Gültigkeitsdauer der Magnetkarte oder das Abbuchen eines bestimmten Betrages von einem Kartenguthaben durchgeführt werden. Die manipulierten Rohdaten werden dann wieder auf die Magnetkarte zurückgeschrieben. Dabei steuern die Informationen, die zum Entschlüsseln der Daten benutzt wurden, die Stärke des Schreibstromes des Schreibkopfes. In den Bereichen hoher Koerzitivität des Magnetstreifens muß dabei mit einem höheren Schreibstrom gearbeitet werden als in den Bereichen niedriger Koerzitivität. Damit können nur solche Magnetkarten beschrieben werden, deren Entschlüsselungsinformation vorher auch ermittelt worden sind.

Damit sind die manipulierten Rohdaten abhängig von Position und Ausdehnung des Musters und der Koerzitivität des Magnetstreifens auf der Magnetkarte verschlüsselt gespeichert.

Die Voraussetzung für ein Beschreiben derartiger Magnetkarten ist ein Lese-/Schreibkopf in einem Magnetkarten-Lesegerät, dessen Schreibstrom steuerbar ist. Außerdem müssen Magnetkarten, die mit einem solchen beliebigen Muster versehen sind, vor dem ersten Lesevorgang, vorzugsweise bereits ab Werk, mit Daten beschrieben sein. Dabei ist nicht der Inhalt dieser Daten wichtig, sondern vielmehr die Tatsache, daß sie auf den Magnetstreifen mittels periodischer Flußwechsel abgelegt sind. Diese Flußwechsel werden zum Lokalisieren der Position und Ausdehnung des magnetischen Musters auf dem Magnetstreifen und zur Bestimmung der Koerzitivität des Magnetstreifens benötigt. Aus diesen Angaben werden die Entschlüsselungsinformationen für die jeweilige Magnetkarte extrahiert.

Ein Kopieren der Daten von Magnetkarten durch ein einfaches Lese-/Schreibgerät wird durch die erfindungsgemäß verschlüsselte Magnetkarte unmöglich. Die unterschiedliche Koerzitivität von Muster und Magnetstreifen und das auf nahezu jeder Magnetkarte verschiedene Muster führen dazu, daß die vom Magnetstreifen einer ersten Magnetkarten im Lesekopf induzierte Spannung nicht proportional dem Schreibstrom des Schreibkopfes für den Magnetstreifen einer zweiten Magnetkarte ist. Die von einer ersten Magnetkarte gelesenen Daten werden dadurch falsch auf eine zweite übertragen. Die Folge ist, daß die kopierte Magnetkarte völlig falsche Daten enthält oder ganz unlesbar ist.

Auch ein Kopieren der Magnetkarten durch mittiges Durchschneiden des Magnetstreifens in Längsrichtung wird durch die erfindungsgemäße Verschlüsselung der Daten verhindert. Das Aufbringen eines beliebigen Musters erlaubt es auch, Muster aufzubringen, die asymmetrisch relativ zur Längsachse des Magnetstreifens sind. Das hat zur Folge, daß man durch Längsteilung des Magnetstreifens zwei Magnetstreifen mit unterschiedlichen magnetischen Mustern erhält. Mit hoher Wahrscheinlichkeit sind die beiden halben Magnetstreifen mit den darauf enthaltenen Daten unlesbar. Dies kommt daher, daß die Daten ursprünglich mit den Entschlüsselungsinformationen, die aus dem gesamten Magnetstreifen ermittelt wurden, gespeichert wurden. Beim Einlesen eines halben Magnetstreifens werden sich nun aufgrund der unterschiedlichen Position und Ausdehnung des magnetischen Musters andere Entschlüsselungsinformationen ergeben, mit denen die ursprünglich auf der Magnetkarte abgelegten Daten nicht entschlüsselbar sind.

Eine bevorzugte Ausführungsform der Erfindung sieht vor, daß die Koerzitivität des magnetischen Materials des Musters ein Mehrfaches der Koerzitivität des Magnetstreifens aufweist.

Zwischen der Koerzitivität des magnetischen Materials des Musters und der Koerzitivität des Materials des Magnetstreifens besteht ein deutlicher Unterschied. Dadurch wird es ermöglicht, daß das Muster eindeutig von dem Magnetstreifen unterschieden werden kann. Möglicherweise bei der Lokalisation des magnetischen Musters auftretende Probleme aufgrund eines zu geringen Unterschiedes zwischen der Koerzitivität des Musters und der des Magnetstreifens werden so vermieden. Die Anzahl der unlesbaren oder fehlerhaft verschlüsselten Magnetkarten wird auf ein Minimum reduziert.

Weitere Ausführungsformen der Erfindung sehen vor, daß das beliebige Muster eine zufällige oder eine geordnete Form aufweist.

Das Muster wird durch unterschiedliche magnetische Materialien auf dem Magnetstreifen aufgebracht. Denkbar sind beispielsweise magnetische Dispersionen, magnetische Späne oder Folien aus magnetischen Materialien. Die Form des Musters kann dabei dem Zufall unterliegen oder aber geordnete Formen aufweisen. Solche geordneten Formen des magnetischen Musters sind beispielsweise geometrische Formen oder Buchstabenkombinationen.

Bei beiden Formen des magnetischen Musters muß allerdings darauf geachtet werden, daß der Magnetstreifen und das magnetische Muster eine einheitliche Farbe aufweisen, um zu verhindern, daß die Position und Ausdehnung des magnetischen Musters von außen optisch sichtbar ist und daraus die Informationen zur Entschlüsselung der Daten gewonnen werden können. Es ist jedoch denkbar, beispielsweise zu Werbezwecken, zusätzlich zum magnetischen Muster in der Farbe des Magnetstreifens ein weiteres farbiges Muster in Form eines Firmenlogos oder einer Buchstabenkombination in einer Farbe anzubringen, die sich von der Farbe des Magnetstreifens unterscheidet.

Im folgenden soll die Erfindung anhand einer Zeichnung und eines Flußdiagrammes näher erläutert werden. Es zeigen:

Fig. 1 eine Ausführungsform der erfindungsgemäß verschlüsselten Magnetkarte;

Fig. 2 ein Flußdiagramm zum Entschlüsseln und Wiederverschlüsseln der Daten auf einer erfindungsgemäß verschlüsselten Magnetkarte.

In **Fig. 1** ist eine Magnetkarte mit der Bezugsziffer **1** gekennzeichnet. Auf einem Trägermaterial **2** ist ein Magnetstreifen **3** aufgebracht. Das Trägermaterial **2** besteht beispielsweise aus Papier oder Kunststoff. Zum Verschlüsseln der auf dem Magnetstreifen gespeicherten Daten wird dieser mit einem magnetischen Muster **4, 5** versehen. Das Muster **4, 5** besteht beispielsweise aus magnetischen Spänen, magnetischer Dispersion oder Folie aus magnetischen Materialien und wird auf dem Magnetstreifen **3** aufgebracht. Das magnetische Muster **4, 5** kann beliebige Formen haben. Das Muster **4** hat eine zufällige Form, wohingegen das Muster **5** eine geordnete Form, beispielsweise eine Buchstabenkombination, aufweist.

In **Fig. 2** ist ein Flußdiagramm dargestellt, welches die verschiedenen Schritte beim Entschlüsseln und Verschlüsseln der Daten auf dem Magnetstreifen einer erfindungsgemäß verschlüsselten Magnetkarte näher erläutert. Als erstes werden die Position und die Ausdehnung des magnetischen Musters auf dem Magnetstreifen und die Koerzitivität des Magnetstreifens abhangig vom Flußwechsel ermittelt. Aus diesen Angaben werden die Entschlüsselungsinformationen extrahiert. Mit Hilfe dieser Entschlüsselungsinformationen werden aus den eingelesenen, verschlüsselten Daten die Rohdaten ermittelt. Diese Rohdaten werden dann aufgrund externer Ereignisse manipuliert; beispielsweise wird die Gültigkeitsdauer der Magnetkarte verlängert. Diese manipulierten Rohdaten müssen dann wieder auf die Karte geschrieben werden. Mit Hilfe der Entschlüsselungsinformationen werden die Rohdaten wieder verschlüsselt und durch entsprechendes Steuern des Schreibstromes eines Schreibkopfes auf dem Magnetstreifen der Magnetkarte abgespeichert.

Patentansprüche

1. Magnetisches Speichermedium, insbesondere eine Magnetkarte (1) mit einem Magnetstreifen (3), auf dem Rohdaten mit einem bestimmten Informa-

tionsgehalt in verschlüsselter Form abgespeichert sind, **dadurch gekennzeichnet,** daß auf dem Magnetstreifen (3) ein beliebiges Muster (4, 5) aus einem magnetischen Material mit einer von der Koerzitivität des Magnetstreifens (3) abweichenden Koerzitivität aufgebracht ist.

2. Magnetisches Speichermedium nach Anspruch 1, dadurch gekennzeichnet, daß die Koerzitivität des magnetischen Materials des Musters (4, 5) ein Mehrfaches der Koerzitivität des Magnetstreifens (3) aufweist.

3. Magnetisches Speichermedium nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das beliebige Muster (4, 5) eine zufällige Form (4) aufweist.

4. Magnetisches Speichermedium nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß das beliebige Muster (4, 5) eine gezielte Form (5) aufweist.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 35 019 A1
Int. Cl.[6]: G 11 B 5/70
Offenlegungstag: 27. März 1997

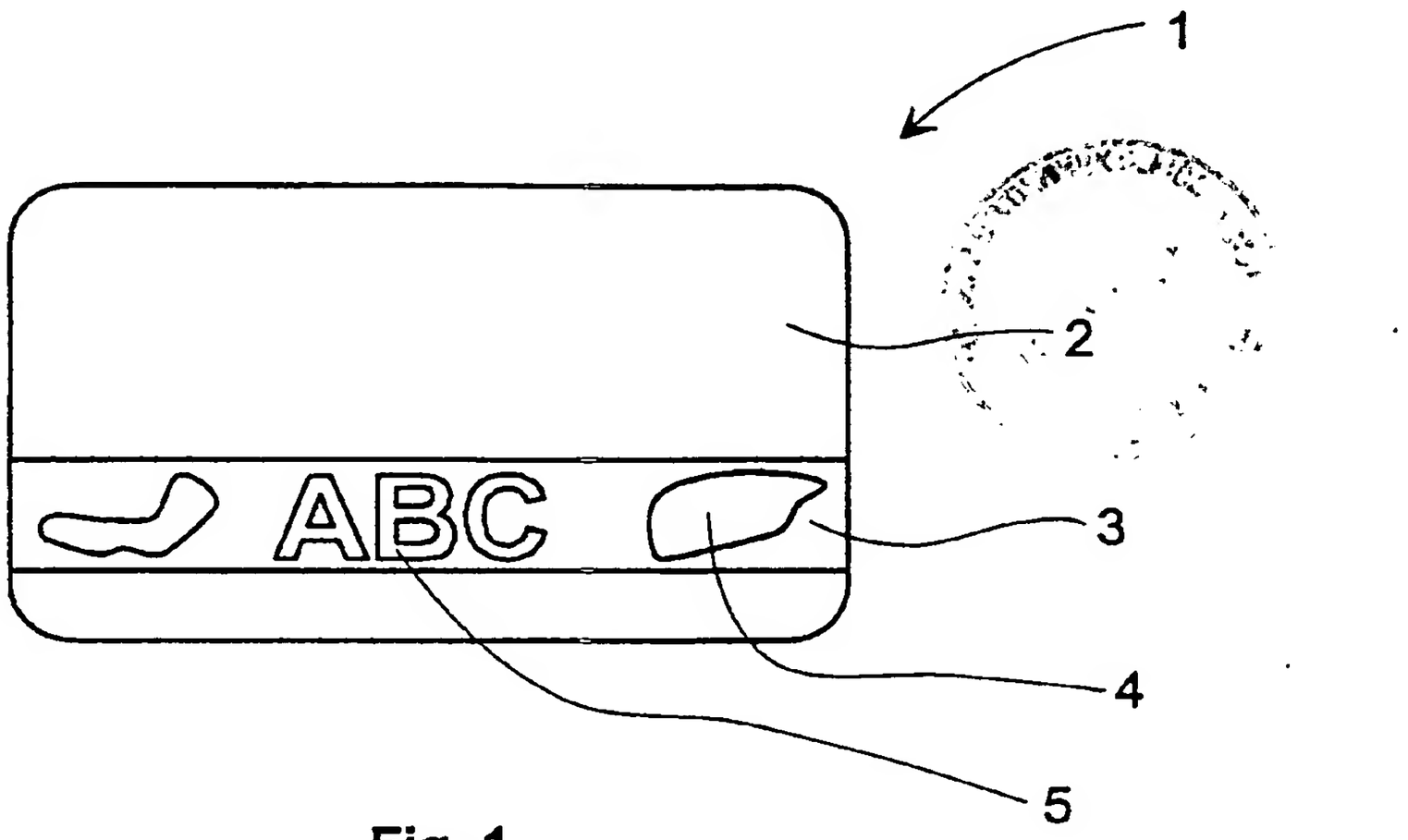


Fig. 1

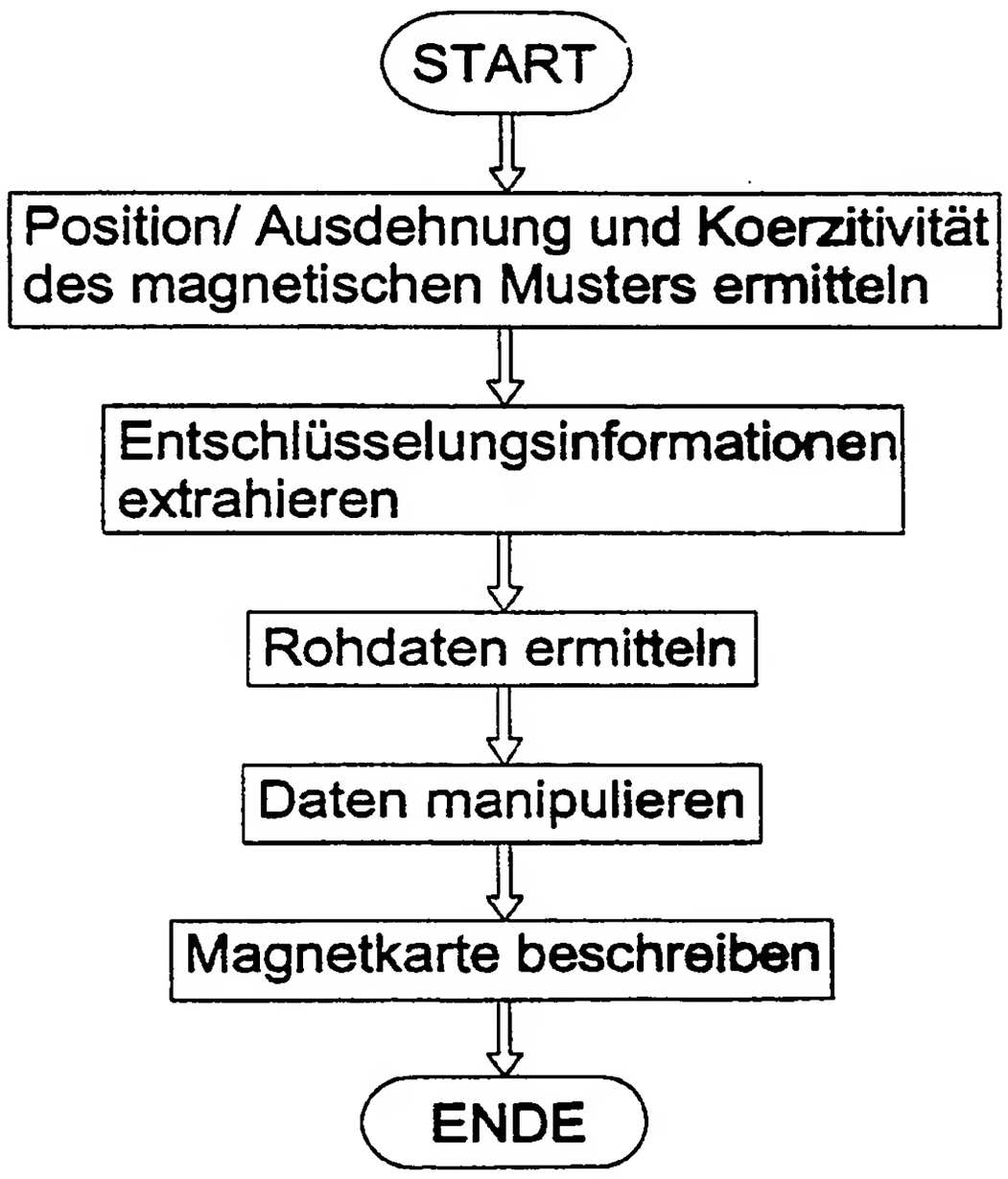


Fig. 2